CLAIMS

I claim:

Sub B1

1. A method of generating block substitution tables for a predetermined block size, comprising:

selecting a first generating function;

selecting a second generating function;

selecting first and second sets of complete linearly independent numbers;

calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers; and

creating nonlinear block substitution tables by combining the linear orthomorphisms, the block substitution tables for use in encrypting clear text messages.

2. The method of claim 1, wherein selecting a first generating function includes selecting a first primitive generating function.

3. The method of claim1, wherein selecting a first generating function includes selecting a first non-primitive generating function.

4. The method of claim 1, wherein selecting a second generating function includes selecting a second primitive generating function.

5. The method of claim1, wherein selecting a second generating function includes selecting a second non-primitive generating function.

6. The method of claim 5, wherein selecting a second non-primitive generating function includes selecting a second non-primitive generating function having a cycle pattern that is identical to a cycle pattern of the first generating function.

7. The method of claim 1, wherein calculating first and second linear orthomorphisms includes calculating first and second maximal linear orthomorphisms from the generating functions and the sets of linearly independent numbers.

8. The method of claim 1, further comprising rotating the second linear orthomorphism.

9. The method of claim 8, wherein rotating the second linear orthomorphism includes rotating corresponding cycles of the second linear orthomorphism.

10. The method of claim 1, wherein selecting a second generating function includes selecting a second generating function which is a complement of the first generating function.

11. The method of claim 1, wherein selecting a second generating function includes selecting a second generating function which is any generating function that is not identical to the first generating function and has a cycle structure which matches a cycle structure of the first generating function.

12. The method of claim 1, wherein selecting first and second sets of linearly independent numbers includes selecting a second set of linearly independent numbers that is identical to the first set of linearly independent numbers.

13. The method of claim 1, wherein selecting first and second sets of linearly independent numbers includes selecting a second set of linearly independent numbers that is not identical to the first set of linearly independent numbers.

14. The method of claim 1, further comprising determining whether all cycles of the first and second linear orthomorphisms are self-contained.

15. The method of claim 14, further comprising selecting pairs of cycles from the first and second linear orthomorphisms to produce a mapping for which $N(x,y)\neq 0$ for all pairs of numbers from different cycles.

16. A computer-implemented method for generating nonlinear block substitution tables from binary data, comprising:

selecting a first set of a plurality of complete linearly independent numbers from the binary data;

selecting a second set of a plurality of complete linearly independent numbers from the binary data;

generating a plurality of linear orthomorphisms using first and second recursive generating functions and the first and second sets of linearly independent numbers; and

setting the substitution tables based on a combination of the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of a sequence of binary numbers.

17. The method of claim 16, wherein the second generating function is a complement of the first generating function.

18. A computer-implemented method for generating nonlinear block substitution tables from binary data, comprising:

selecting a first set of a plurality of complete linearly independent numbers from the binary data;

selecting a second set of a plurality of complete linearly independent numbers from the binary data;

recursively applying a first generating function to the first set of linearly independent numbers to create a major cycle of a first orthomorphism;

generating a plurality of cycles of the first orthomorphism;

recursively applying a second generating function to the second set of linearly independent numbers to create a major cycle of a second orthomorphism;

generating a plurality of cycles of the second orthomorphism; and

setting the substitution tables by combining the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of an ordering of binary numbers.

19. The method of claim 18, wherein the second generating function is a complement of the first generating function.

20. A system, comprising:

a communications link;

a first computer in communication with the communications link; and

a second computer in communications with the communications link, the second computer having an ordered set of data and instructions stored thereon which, when executed by the second computer, cause the second computer to perform the steps of:

selecting a first generating function;

selecting a second generating function;

selecting first and second sets of complete linearly independent numbers;

calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers; and

creating nonlinear block substitution tables by combining the linear orthomorphisms, the block substitution tables for use in encrypting clear text messages.

21. A computer-readable medium having stored thereon instructions which, when executed by a processor, cause the processor to perform the steps of:

selecting a first generating function;

selecting a second generating function;

selecting first and second sets of complete linearly independent numbers;

calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers; and

creating nonlinear block substitution tables by combining the linear orthomorphisms, the block substitution tables for use in encrypting clear text messages.

22. An apparatus, comprising:

means for selecting a first generating function;

means for selecting a second generating function;

means for selecting first and second sets of complete linearly independent numbers;

means for calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers; and

means for creating nonlinear block substitution tables by combining the linear orthomorphisms, the block substitution tables for use in encrypting clear text messages.